CLAIMS

We claim:

1. A computer-readable medium containing an identity certificate data structure, the identity certificate data structure comprising:

a first data field containing data representing an identity peer name;

a second data field containing data representing an identity public key, the identity public key and an identity private key forming a public/private key pair;

a third data field containing data representing a certificate type, the certificate type indicating an identity certificate; and

a fourth data field containing data representing a signature of the identity certificate, the signature derived, at least in part, from the identity private key.

2. The identity certificate data structure of claim 1 wherein the identity certificate data structure is an X.509 certificate.

3. The identity certificate data structure of claim 2 wherein the first data field is a subject alternative name field of the X.509 certificate.

4. The identity certificate data structure of claim 2 wherein the third data field is an extension property field of the X.509 certificate.

5. The identity certificate data structure of claim 1 wherein the identity peer name in the first data field is globally unique.

6. The identity certificate data structure of claim 1 wherein the identity peer name in the first data field is derived, at least in part, from the identity public key in the second data field.

7. The identity certificate data structure of claim 6 wherein the identity peer name in the first data field is derived, at least in part, from a hash of the identity public key in the second data field.

8. The identity certificate data structure of claim 1 wherein the identity private key is stored in a Cryptographic Service Provider container.

9. The identity certificate data structure of claim 1 further comprising:

a fifth data field containing data representing an issuer of the identity certificate; and

a sixth data field containing data representing a subject of the identity certificate, wherein the issuer and the subject of the identity certificate are the same.

10. The identity certificate data structure of claim 1 further comprising:

a fifth data field containing data representing a period of validity of the identity certificate.

11. The identity certificate data structure of claim 1 further comprising:

a fifth data field containing data representing a version of the identity certificate.

12. A computer-readable medium containing a group root certificate data structure, the group root certificate data structure comprising:

a first data field containing data representing a group peer name;

a second data field containing data representing a group root public key;

a third data field containing data representing a certificate type, the certificate type indicating a group root certificate; and

a fourth data field containing data representing a signature of the group root certificate, the signature derived, at least in part, from a group root private key, the group root private key and the group root public key in the second data field forming a public/private key pair.

13. The group root certificate data structure of claim 12 wherein the group root certificate data structure is an X.509 certificate.

14. The group root certificate data structure of claim 13 wherein the first data field is a subject alternative name field of the X.509 certificate.

15. The group root certificate data structure of claim 13 wherein the third data field is an extension property field of the X.509 certificate.

16. The group root certificate data structure of claim 12 wherein the group peer name in the first data field is globally unique.

17. The group root certificate data structure of claim 12 wherein the group peer name in the first data field is derived, at least in part, from the group root public key in the second data field.

18. The group root data structure of claim 17 wherein the group peer name in the first data field is derived, at least in part, from a hash of the group root public key in the second data field.

19. The group root certificate data structure of claim 12 further comprising:

a fifth data field containing data representing an issuer of the group root certificate; and

a sixth data field containing data representing a subject of the group root certificate, wherein the issuer and the subject of the group root certificate are the same.

20. The group root certificate data structure of claim 12 further comprising:

a fifth data field containing data representing a period of validity of the group root certificate.

21. The group root certificate data structure of claim 12 further comprising:

a fifth data field containing data representing a version of the group root certificate.

22. A computer-readable medium containing a group membership certificate data structure, the group membership certificate data structure comprising:

a first data field containing data representing a group peer name;

a second data field containing data representing an issuer peer name;

a third data field containing data representing a subject peer name;

a fourth data field containing data representing a certificate type, the certificate type indicating a group membership certificate; and

a fifth data field containing data representing a signature of the group membership certificate.

23. The group membership certificate data structure of claim 22 wherein the group membership certificate data structure is an X.509 certificate.

24. The group membership certificate data structure of claim 23 wherein the first data field is an extension property field of the X.509 certificate.

25. The group membership data structure of claim 23 wherein the second data field is an issuer alternative name field of the X.509 certificate.

26. The group membership data structure of claim 23 wherein the third data field is a subject alternative name field of the X.509 certificate.

27. The group membership data structure of claim 22 wherein the group peer name in the first data field is globally unique.

28. The group membership data structure of claim 22 wherein the issuer peer name in the second data field is a reference to a certificate selected from the group consisting of: a group root certificate and a group membership certificate.

29. The group membership certificate data structure of claim 22 further comprising:

a sixth data field containing data representing a period of validity of the group membership certificate.

30. The group membership certificate data structure of claim 22 further comprising:

a sixth data field containing data representing a version of the group membership certificate.

31. The group membership certificate data structure of claim 22 further comprising:

a sixth data field containing data representing a public key, the public key and a private key forming a public/private key pair.

32. A computer-readable medium containing a group certificate chain data structure, the group certificate chain data structure comprising:

a first data field containing data representing a group root certificate, the group root certificate comprising:

a second data field containing data representing a group peer name;

a third data field containing data representing a group root public key;

a fourth data field containing data representing a certificate type, the certificate type indicating a group root certificate; and

a fifth data field containing data representing a signature of the group root certificate, the signature derived, at least in part, from a group root private key, the group root private key and the group root public key in the third data field forming a public/private key pair; and

a sixth data field containing data representing a group membership certificate, the group membership certificate comprising:

a seventh data field containing data representing a group peer name, the group peer name in the seventh data field being the same as the group peer name in the second data field in the group root certificate;

an eighth data field containing data representing an issuer peer name, the issuer peer name in the eighth data field being a reference to the group root certificate in the first data field;

a ninth data field containing data representing a subject peer name;

a tenth data field containing data representing a certificate type, the certificate type indicating a group membership certificate; and

an eleventh data field containing data representing a signature of the group membership certificate.

33. The group certificate chain data structure of claim 32 wherein the group root certificate and the group membership certificate are X.509 certificates.

34. The group certificate chain data structure of claim 32 wherein the group membership certificate in the sixth data field further comprises:

a twelfth data field containing data representing a public key, the key and a private key forming a public/private key pair.

35. The group certificate chain data structure of claim 34 further comprising:

a thirteenth data field containing data representing a second group membership certificate, the second group membership certificate comprising:

a fourteenth data field containing data representing a group peer name, the group peer name in the fourteenth data field being the same as the group peer name in the second data field in the group root certificate;

a fifteenth data field containing data representing an issuer peer name, the issuer peer name in the fifteenth data field being a reference to the group membership certificate in the sixth data field;

a sixteenth data field containing data representing a subject peer name;

a seventeenth data field containing data representing a certificate type, the certificate type indicating a group membership certificate; and

an eighteenth data field containing data representing a signature of the second group membership certificate.